Integration of a Bayesian network for response planning in a maritime piracy risk management system

Xavier Chaze, Amal Bouejla, Aldo Napoli, Franck Guarnieri

Integration of a Bayesian network for response planning in a maritime piracy risk management system

Chaze X.
MINES ParisTech - CRC
BP 207. 1 Rue Claude Daunesse
06904 Sophia Antipolis Cedex, France
xavier.chaze@mines-paristech.fr

Bouejla A., Napoli A., Guarnieri F.
MINES ParisTech - CRC
BP 207. 1 Rue Claude Daunesse
06904 Sophia Antipolis Cedex, France.
amal.bouejla@mines-paristech.fr
aldo.napoli@mines-paristech.fr
franck.guarnieri@mines-paristech.fr

Abstract - *This article describes an innovative system to protect offshore oil infrastructure against maritime piracy. To detect and respond efficiently to this threat, many factors must be taken into account, including the potential target, the protection methods already in place and operational and environmental constraints, etc. To improve the handling of this complex issue, we have designed a system to manage the entire processing chain; from threat identification to implementation of the response. The system implements Bayesian networks in order to capture the multitude of parameters and their inherent uncertainties, and to identify and manage potential responses. This article describes the system architecture, the integrated Bayesian network and its contribution to response planning.*

Keywords: Maritime piracy, Oil platforms, SARGOS, Bayesian networks, International Maritime Organisation, Expert knowledge.

1 Presentation of the SARGOS system

1.1 Context

Offshore oil extraction currently accounts for about one-third of global oil production. Despite its scarcity, this source of energy is under active exploration in many parts of the world, notably in hazardous territorial waters such as the Gulf of Guinea, and particularly off the Nigerian coast.

Since 2005, the number of acts of piracy against oil fields and especially ships has grown steadily (in 2011, 552 attacks on ships and platforms were registered with the International Maritime Bureau[1]). Attacks on infrastructure generate significant additional costs arising from the payment of ransoms, the installation of security equipment, and increased insurance premiums, etc. These additional costs directly affect the international price of oil [1] and [2]. Although attacks on oil platforms are less frequent and certainly less publicised, they are extremely disturbing because of the severe impact on the crew (personnel may be taken hostage, injured or even killed), infrastructure (facilities may be damaged or destroyed), the economy (price spikes) and the environment (oil spills). The lack of effective tools for infrastructure protection means that actors involved in the offshore oil and gas industry find themselves helpless. One example is the attack on the Exxon Mobil platform [3] off the coast of Nigeria, which led to the kidnapping of nineteen employees and extensive damage to the facility caused by the explosive devices used by the pirates. Such incidents are prime examples of the weaknesses in current anti-piracy systems. At the present time, oil installation security is provided by so-called classical tools (radio identification, radar, Automatic Identification Systems, etc.), which, despite their usefulness in detection, cannot provide a response tailored to different types of threats (fishing boat, jet ski, etc.). Moreover, their effectiveness depends on many parameters related to both the environment and technical and operational constraints.

1.2 SARGOS objectives

To meet this new need for the protection of civilian infrastructure, the French National Research Agency (ANR) has funded the SARGOS[2] system. The project is approved by French regional bodies and brings together a multi-disciplinary consortium[3] of partners with complementary skills. The aim is to design a system to improve infrastructure protection and offer a new method that is able to both detect threats and plan a response because at the present time, there is no comprehensive system capable of managing the entire threat processing chain.

[1] International Chamber of Commerce International Maritime Bureau's Piracy Reporting Centre (http://www.icc-ccs.org)

[2] Graduated Offshore Response and Alert System (*Système d'Alerte et de Réponse Graduée OffShore*).

[3] The SARGOS project includes participants from private sector organisations such as DCNS (a French naval shipbuilder) and SOFRESUD (a supplier of high-tech equipment to the defence industry), and public research centres including ARMINES (a French contract research organisation) and TéSA (Telecommunications for Space and Aeronautics).

Chaze X., Bouejla A., Napoli A. et Guarnieri F., 2012 :
« Integration of a Bayesian network for response planning in a maritime piracy risk management system »,
Conférence internationale IEEE SOSE 2012 (7th International Conference on System Of Systems Engineering), Gênes, Italie, 16-19 juillet 2012

To achieve this, the system must be capable, in the case of a confirmed intrusion, of generating an alarm and initiating an internal and external response appropriated to the danger level of the situation. This response has to be implemented through a graduated series of non-lethal counter-measures (sonic cannons, barring infrastructure access, etc.).

1.3 System architecture

The SARGOS system architecture consists of two major sub-systems. First, a module for the detection, tracking and classification of threats in the marine environment: using powerful instrumentation (FMCW[4] radar, infrared cameras, etc.) the SARGOS system can identify a potential intrusion and generate an alert report that provides an inventory of all the relevant parameters necessary to characterise the threat. And a module to formalise and model graduated responses: taking into account the evolution of the situation, regulatory constraints and the operational infrastructure, the data contained in the alert report just described is used to define an appropriate response to deter or repel attackers.

The functional diagram of the SARGOS system demonstrates this threat processing cycle (Figure 1).

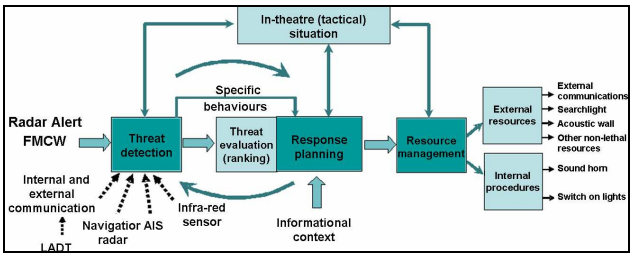


Figure 1. Functional diagram of the SARGOS system

The safety and security of the infrastructure is assured by the application of a response plan generated by the system, which triggers a series of progressive and reversible actions and reactions.

2 Contribution of a Bayesian network

Actually, the great weakness in this process lies in the preparation of the diagnosis used for planning the response. To overcome this shortcoming, we propose a new approach that is able to generate automated response plans, tailored to the nature of the detected intrusion.

2.1 Why a Bayesian network?

A detailed investigation of the issues highlights significant constraints that the SARGOS system must take into account in order to fully reflect the complexity of a situation [4]. On the one hand, the large number of variables to be included (representing the threat, the target, the environment, etc.) and the dependencies that may exist between them suggest the development of a decision support system based on graph theory. On the other hand, the uncertainty inherent in certain variables (threat identification, intervention options, etc.) emphasises the need for a system based on probability theory and probabilistic calculations [5]. With these two approaches in mind, a process for the automatic preparation of response plans tailored to the nature of the detected intrusion, based on Bayesian networks was explored [6] and [7].

We focus particularly on the contribution of Bayesian inference techniques that are applied to, on the one hand, a maritime database and on the other to expert knowledge in the domains of offshore oil and maritime safety. Data from the database and expert knowledge are modelled using Bayesian networks, tools based on Thomas Bayes' theorem (1).

$$P(A/B) = \frac{P(B/A)\,P(A)}{P(B)} \qquad (1)$$

The theorem is used in statistical inference to update probability estimates from observations and the probability distributions applicable to these observations. A Bayesian network represents knowledge in a way that makes it possible to calculate conditional probabilities [8]. Widely used for diagnosis (medical or industrial), Bayesian networks capitalise and exploit knowledge, and are particularly suitable for capturing and reasoning with uncertainty inherent in many complex problems [9], [10] and [11].

2.2 Software used

Among the existing softwares specialised in Bayesian networks, it was decided to choose the Bayesia software series which proposes on one hand an intuitive desktop solution that experts have easily learned to use in a very short time and on the other hand an Application Programming Interface (API) which can include a previously created Bayesian network into a standalone module.

Indeed, BayesiaLab[5] software was first used to automatically generate an initial network (from existing piracy data) by suggesting dependencies between the principal variables [12]. The software was used again in the second stage (by experts) to determine the complete architecture of the final SARGOS network (cf. §2.3).

This desktop version was then used to test the results of the model developed using simulated scenarios. Thanks to the graphical interface, experts can create realistic attack scenarios by determining the modalities of their choice. The

[4] Frequency Modulated Continuous Wave

[5] BayesiaLab software is developed by the French company Bayesia (http://www.bayesia.com/)

Chaze X., Bouejla A., Napoli A. et Guarnieri F., 2012 :
« Integration of a Bayesian network for response planning in a maritime piracy risk management system »,
Conférence internationale IEEE SOSE 2012 (7th International Conference on System Of Systems Engineering), Gênes, Italie, 16-19 juillet 2012

Bayesian network then calculates the resulting probabilities which are analysed by the experts to improve iteratively the initial modalities and probabilities (cf. §3.2).

Finally, the API provided by the Bayesia software series provides an efficient tool to operate an existing Bayesian network automatically and integrate it in a standalone system, making so possible a real-time use (cf. §3.3).

2.3 Implementation method

The approach used to construct the SARGOS Bayesian network consists of two complementary steps. First, an initial Bayesian network was constructed using data from the 'Piracy and Armed Robbery database' of the International Maritime Organisation (IMO[6]). This is the only database in existence that holds historic records of pirate attacks in the maritime environment. On 15th July, 2011 the database contained records of 5,502 attacks (dating back to 1994) and the data noted for each attack included: the name of the asset under attack, the number of attackers, the weapons used, the measures taken by the crew to protect themselves, the impact on the crew and the pirates, etc.

This approach served two purposes: first, it made it possible to determine the principal tools and measures used by the crew to protect themselves, to evaluate their effectiveness and to define the probability of certain types of attack; and secondly it helped to define an initial framework for the formalisation of knowledge related to acts of maritime piracy.

The second step leveraged expert knowledge in the oil and safety domains. As the information contained in the IMO database related primarily to attacks on shipping, the contribution of knowledge from domain experts made it possible to extend the system to include oil fields [13]. Using the Bayesian network created from the IMO data, experts were able to share and transfer knowledge that was then used to build the final Bayesian network and complete the architecture in order to make it as versatile as possible (nodes and arcs were added, modalities and probabilities were modified) [14]. In this way, the data extracted from the IMO database was combined with the experience of experts, through the course of multiple brainstorming sessions, in order to address the a priori lack of knowledge and experiential feedback.

Furthermore, in future, we could also imagine improve our specific knowledge. Once SARGOS systems will be operational on several platforms or offshore infrastructures, all events which will be treated will come enrich a database of existing cases. From this historical data and continuous real-time flow of data, it would be possible to define datamining rules in order to discover new knowledge [15]. These rules will supply an automated reasoning rule-based knowledge to allow the automatic identification of abnormal behavior of vessels typical of a risk of maritime piracy attack.

[6] http://www.imo.org

3 Results and integration in the SARGOS system

3.1 Model developed

The basic architecture of the SARGOS response planning network consists of four modules and five sub-modules (Figure 2).

The modules are: Basic parameters; Aggravating factors and constraints; the Overall danger level of the situation; the Countermeasures. Basic parameters are static or dynamic physical data that characterise the threat and the target. They are either obtained directly from the alert report or are derived from it. Aggravating factors make it possible to take into account the potential deterioration of the situation, while constraints are parameters that must be taken into account to ensure the effectiveness of the response both technically and operationally. The overall danger level of the situation is derived from the basic parameters. Its assessment takes into account the potential consequences of the problem created by the threat and the vulnerability of the target. Countermeasures are all the defences implemented by the target in order to return as quickly as possible, and in the best condition possible, to a safe situation. Countermeasures are classified into five sub-modules according to the danger level of the situation and the operational availability of on-board equipment.

These sub-modules are: Communication and distress calls; Deterrence and low-impact repulsion measures; Repulsion, anti-boarding and neutralisation measures; Procedure management; Ensuring the safety and security of the facility. From these sub-modules, the Bayesian network proposes a set of countermeasures that may be activated according to the estimated danger level (for example: activate the safety system and silent alert, etc.).

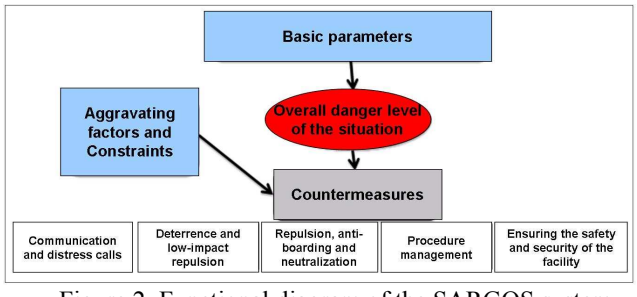


Figure 2. Functional diagram of the SARGOS system

The planning report generated by the network makes it possible to make a rational assessment of probabilities and formalises expert knowledge. This report constitutes the interface between the processing of the alert report and exploitation of the results of the Bayesian network. It is a summary of the essential information needed to actually

trigger response procedures. Consequently the probability of activating a particular countermeasure will obviously vary according to the situation.

3.2 Simulation of attack scenarios

Once the probability distribution of the various modalities has been established, an interesting exercise is to test the Bayesian network by using it to simulate different attack scenarios through the selection of certain criteria. An examination of these scenarios made it possible to finalise the network before integrating it into the SARGOS system.

The example below (Figure 3) shows how response planning is tailored to the danger level of the situation and can adapt to changes in parameters representing the threat and the target. Specifically, it shows the results of setting parameters to simulate an attack on a Floating Production, Storage and Offloading (FPSO) unit by an unknown vessel. This example shows that the danger level of the situation, at time T1, was 2 with a 64.68% probability of occurrence. In this case the counter-measures to be applied were: inform the crew master, request the intervention of the security vessel, broadcast a strong message by loudspeaker, turn on the searchlight and activate the security post.

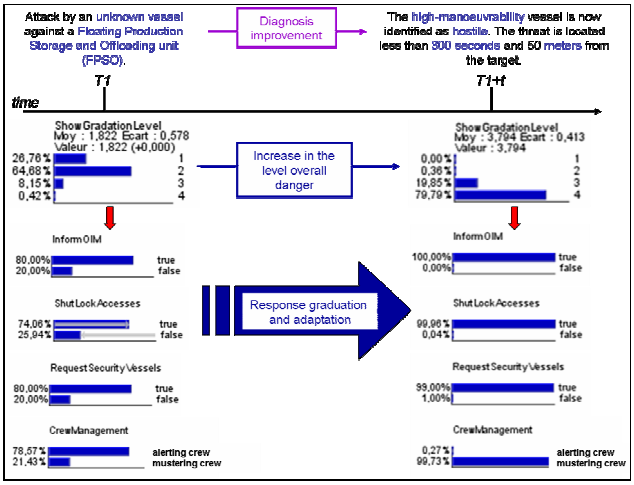


Figure 3. Evolution of response planning as more information about the situation becomes available

At time T1+t the attacker has been identified as hostile and equipped with a highly maneuverable boat. The parameters that impacted response planning were: the ranking between the threat and the target (i.e. the time required for the threat to cover the remaining distance to the target), the distance between the threat and the target and the response time of the security vessel. The danger level is now 4 with a 79.79% probability of occurrence. This higher level requires a more forceful response, reflected in the recommended measures: assemble the crew, secure the installation and block access to sensitive areas.

The creation of attack scenarios makes it possible to refine the probability of an attack and test the response of the Bayesian network by changing the parameters that represent the threat, the target, the environment, etc.

3.3 Integration of the Bayesian network into the SARGOS system

In order to integrate the Bayesian network into the SARGOS system, a prototype was developed that included an alert report as input and a planning report (which listed all the counter-measures to be applied either by the crew or automatically by the system) as output. The BayesiaEngine software provides a module that makes it possible to select and set attack parameters. This module consists of an application programming interface (API) and a Java library. Intermediate calculations are carried out on the basis of these parameters and the results are fed into the enhanced Bayesian network created from expert knowledge.

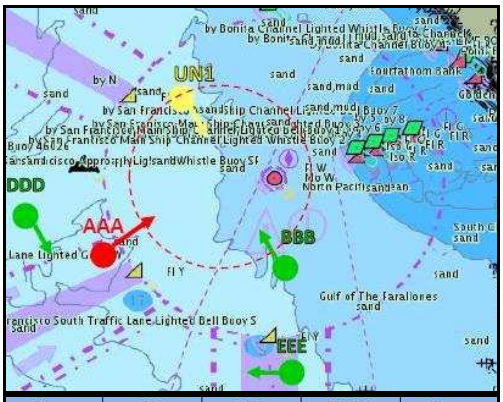
The resulting list of counter-measures varies according to the attack scenario. Consequently, a threshold must be set in order to only activate those measures that provide the most relevant response at a particular time, and in a particular situation. This threshold was set at 70%. In other words, only those counter-measures where one of the modalities had a probability greater than 70% were selected for further processing. This threshold was arrived at by domain experts as it reflects actual events in more than two-thirds of real-life cases. Following an extensive period of testing, the selected counter-measures were found to correspond to realistic and reliable responses.

The SARGOS system can handle multiple threats contained in a single alert report. Consequently, priorities must be established. In the system, the first threat to be treated is always the one where time available to react is the shortest for the target that is most exposed. Figure 4 shows the user interface of the SARGOS system, and demonstrates how multiple threats can be processed simultaneously.

In this example, the system has detected several potential threats heading towards the oil field and has classed them into ‘Enemy’, ‘Unknown’ or ‘Friend’. An alert is only generated following a classification of Enemy or Unknown.

Once a threat has been detected and analysed, the counter-measures are selected and added to the response planning report prepared in a specific order. The main factors determining this order of priority were: the action mode of the counter-measure, its ease of implementation, the degree of automation or the need for a large number of crew members to activate it, the time required for it to become effective and its potential additional functions.

Chaze X., Bouejla A., Napoli A. et Guarnieri F., 2012 :
« Integration of a Bayesian network for response planning in a maritime piracy risk management system »,
Conférence internationale IEEE SOSE 2012 (7th International Conference on System Of Systems Engineering), Gênes, Italie, 16-19 juillet 2012



Class	ID	CPA	TCPA	Type
Enemy	AAA	2. 3 m	3. 30 mn	Small Boat
Unknown	UN1	1.5 m	2.20 mn	
Friend	BBB	2.8 m	4.15mn	Tanker
Friend	CCC	0		Tanker
Friend	DDD	0		Small boat

Figure 4. The user interface of the SARGOS system showing threat prioritisation

The planning report is divided into two parts: the first concerns communication and a general request for assistance directed at the entire oil field; the second concerns the specific asset at risk. The response planning report also displays the counter-measures to be activated in chronological order.

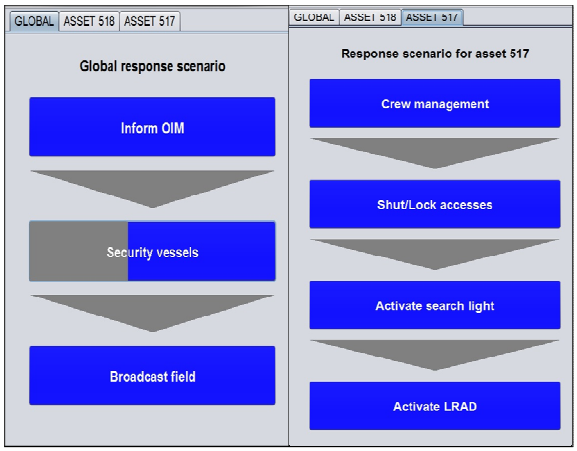


Figure 5. The SARGOS user interface showing global (left-hand side) and specific (right-hand side) countermeasures to be deployed

In the above example (Figure 5) the global counter-measures are, in order: inform the crew master, request the intervention of the security vessel and broadcast information about the attack to other installations in the field. The specific measures are: assemble the crew, block access to the infrastructure, activate searchlights and activate the noise cannon (Long Range Acoustic Device; LRAD). The representation of the probability that a particular measure will be implemented can be seen in the counter-measure 'Security Vessels', where the proportion of the blue segment suggests a 60-70% probability that this method will be called upon.

4 Conclusions

Response planning in the SARGOS system results in the preparation of a response planning report based on an intelligent assessment of the alert report. The response planning report includes all the information necessary for the physical implementation of measures to protect against a threat.

Using a Bayesian network for response planning is a major benefit of the SARGOS system as the network is able to manage all possible interactions between threat characteristics, the target, the environment, the crew and the facilities. It can adapt to real-time changes in the danger level of the situation.

Network scalability is also made possible through integration of feedback related to the processing of attacks previously managed by the system. The planning module can therefore be updated and improved iteratively.

Finally, in order to improve the modeling of knowledge embedded in the Bayesian network, an interesting approach would be to draw upon an appropriate ontology [16]. The use of a suitable ontology would make it possible to formalise knowledge upstream of the Bayesian network in order to consolidate the steps of threat detection and identification.

References

[1] One Earth Future, (2011) "The Economic Cost of Piracy". [online]. Available from http://oneearthfuture.org/images/imagefiles/11%2001%20OBP-Brochure-A4.pdf (Accessed 15 May 2012)

[2] L'Institut Supérieur d'Economie Maritime, (2010) "Piraterie: perturbation de l'économie maritime ? [Piracy: Disruption to the Maritime Economy?]" [online]. Mer et Marine, October 2010. Available from http://www.meretmarine.com/article.cfm?id=114482 (Accessed 15 May 2012)

[3] M.A. Giraud, B. Alhadef, F. Guarnieri, A. Napoli, M. Bottala Gambetta, D.Chaumartin, M. Philips, M. Morel, C. Imbert, E. Itcia, D. Bonacci, P. Michel, (2011) "SARGOS: Securing Offshore Infrastructures Through a Global Alert and Graded Response", System Workshop MAST Europe, June 27-29 2011

[4] B.S. Ware, A.F. Beverina, L. Gong, B. Colder, (2002) "A Risk-Based Decision Support System for Antiterrorism", *Digital Sandbox*, 8 pages, August 14 2002

[5] S. Scott, “A Bayesian paradigm for designing intrusion detection systems”, (2004) *Computational Statistics & Data Analysis*, vol. 45, no. 1, p. 69–83, 2004.

[6] R. Dantu and P. Kolan, (2005) “Risk management using behavior based bayesian networks”. *Intelligence and Security Informatics*, Vol. 3495, pp. 115-126.

[7] L.D. Hudson, B.S. Ware, S.M. Mahoney and K.B. Laskey, (2002) “An Application of Bayesian Networks to Antiterrorism Risk Management for Military Planners”. [online] Available at http://digilib.gmu.edu:8080/jspui/bitstream/1920/268/1/Antiterrorism.pdf (Accessed 15 May 2012)

[8] P. Naïm, P.H. Wuillemin, P. Leray, O. Pourret and A. Becker, (2007), *Réseaux bayésiens*. [*Bayesian Networks*], 3rd ed., Eyrolles.

[9] P.R. Kannan, (2007) “Bayesian networks: Application in safety instrumentation and risk reduction”. *ISA Transactions*, Vol. 46 No 2, April 2007, pp. 255-259.

[10] C.J. Lee and K.L. Lee, (2006) “Application of Bayesian network to the probabilistic risk assessment of nuclear waste disposal”. *Reliability Engineering & System Safety*, Vol. 91 No 5, May 2006, pp. 515-532.

[11] J.E. Martín, T. Rivas, J.M. Matías, J. Taboada and A. Argüelles, (2009) “A Bayesian network analysis of workplace accidents caused by falls from a height”. *Safety Science*, Vol. 47 No. 2 February 2009, pp. 206-214

[12] SûretéGlobale.org, (2008) “Apport des réseaux bayésiens dans la prévention de la délinquance. [The Contribution of Bayesian Networks to Crime Prevention]”. [online]. Available from http://www.sureteglobale.org/pdf/reseaux%20bayesiens.pdf (Accessed 15 May 2012)

[13] X. Chaze, A. Bouejla, A. Napoli, F. Guarnieri, T. Eude et B. Alhadef, (2012) “The Contribution of Bayesian Networks to Manage Risks of Maritime Piracy against Oil Offshore Fields”, in ITEMS 2012 (Information Technologies for the Maritime Sector), Busan, South Korea, *Database Systems for Advanced Applications*, Lecture Notes in Computer Science Volume 7240, 2012, pp 81-91

[14] L. Torti and P.H. Wuillemin, (2009) “Modélisation de réseaux bayésiens de très grandes tailles [Large Scale Bayseian Network Modelling]” in MajecSTIC, 16-18 November 2009, Avignon, France.

[15] B. Idiri, A. Napoli, (2012) « Découverte de règles d'association pour l'aide à la prévision des accidents maritimes », in Conférence Internationale Francophone sur l'Extraction et la Gestion de Connaissance (EGC 2012), Bordeaux, France, *Revue des Nouvelles Technologies de l'Information* RNTI-E-23[2], Editions Hermann, pp 243-248.

[16] A. Vandecasteele and A. Napoli, (2012) “Spatial ontologies for detecting abnormal maritime behaviour” in OCEANS 2012, 28 May 2012, Yeosu, South Korea.